Consumer and Financial Protection Bureau
Legal Technology and Support Team
Privacy Impact Assessment
July 2024

Appendix A

Legal Technology and Support Team

External Evidence Management System/Contract Services

Background

The Consumer Financial Protection Bureau (CFPB) Office of Enforcement (Enforcement) maintains a team of eDiscovery professionals to manage the discovery process in litigation and investigations. Discovery is the process of identifying, preserving, collecting, reviewing, analyzing, and producing information during an investigation or during administrative or civil actions. eDiscovery is simply the extension of this well-established process to the Electronically-Stored Information (ESI) that an organization might possess, including email, instant, messages, word processing files, spreadsheets, presentations, social networking content, voice and audio recordings, content stored in databases or collaboration systems, and all the devices on which this information might be stored.

Professional litigation support products/tools and services help to support several functions related to investigation and litigation. These tools and services enable the litigator to control and manage much larger volumes of case materials, and much more complex information, much more quickly, and to much greater effect, than would otherwise be possible. For example, these tools ingest, analyze, process, format, and organize bureau records for search, retrieval, review, correlation, flagging, and presentation in various data formats (e.g., Microsoft Word and Microsoft Excel), allowing document analysis in bulk within a single data file. Users can view metadata within files stored in these varying file formats and identify and eliminate duplicate documents during the review process.

eDiscovery tools provide redaction capabilities which allows for and automates the identification of protected information (e.g., personally identifiable information) by searching for names, phrases, and terms (collectively, "keywords") that are input by the reviewing attorney. This allows the reviewing attorney to customize keywords for each set of documents or cases that may indicate the existence of privileged or protected information. The tool uses that information to automatically flag files that contain those keywords for the attorney, who will review and determine if the files or information therein should be protected from disclosure.

In addition, Enforcement requires the capability to forensically collect data from external entities when immediate access is granted by a court, often in conjunction with a Temporary

Restraining Order. eDiscovery tools allow CFPB Staff[1] to forensically extract data from storage media to use as evidence in legal proceedings and to gather and store information in a secure and forensically sound manner, including electronic and non-electronic (e.g., paper) information. Early case assessment tools are used in conjunction with other tools to process forensically collected data to identify the types of data collected and conduct triage on a large quantity of information to determine what must be reviewed. Finally, other tools provide trial and investigative hearing support. These events require the use of various specialized trial presentation software tools, which display exhibits, either during investigative hearings or at trial for courtroom presentations.

The CFPB employs the Legal Technology Support Team (LTST), which hosts and provides Enforcement with a suite of eDiscovery applications and tools to process and manage these legal activities. LTST's application suite is comprised of these customized commercial off-the-shelf (COTS) tools and cloud-based solutions (on-premises or vendor-owned) to ensure that CFPB can effectively collect, store, process, transmit, and maintain critical information related to CFPB investigations, litigation, and enforcement processes.

To supplement CFPB's eDiscovery workload, Enforcement has procured the services of a federal contractor to provide eDiscovery and litigation support services. Similarly, these services include a wide range of professional litigation support products/tools and services help to support several functions related to investigation and litigation. However, these tools are housed in a contract-owned environment. The CFPB is publishing this Appendix to the LTST Privacy Impact Assessment (PIA) to document and assess the privacy risks associated with maintaining CFPB records in a contractor-owned environment. The support services described in this PIA Appendix are otherwise covered by the LTST PIA. Therefore, PIA Appendix, along with the PIA, provides coverage for the collection, use, sharing, and maintenance of personally identifiable information shared and maintained within the contractor-owned environment.

This PIA Appendix documents the privacy risks associated with housing CFPB records in a contractor-owned environment. The support services described in this PIA Appendix are otherwise covered by the LTST PIA. The categories of individuals and records; the purpose and uses for collection; and associated privacy risks, mitigations, and controls, are identified and covered by the PIA. This PIA Appendix documents the privacy risks associated with housing CFPB records in a contractor-owned environment that are not addressed explicitly by the LTST PIA.

[1] CFPB Staff means all employees, interns, volunteers, consultants, contractors, and detailees assigned to CFPB.

Privacy Risk Analysis

Data Minimization

There is a risk that CFPB records maintained in the contractor-owned environment will be retained for longer than necessary. To mitigate this risk, all CFPB records are transferred electronically to the contractor, except for in rare situations where the original documents are paper-based. In these situations, the original documents are shipped to the contractor for scanning and the paper documents are returned to the CFPB. CFPB mitigates this risk by implementing a process where all electronic documents maintained within the contractor's environment will either be transferred back to CFPB or destroyed three (3) months after the case—also referred to as a matter—is closed. Upon closure of a matter, the CFPB the Contracting Officer's Representative (COR) notifies the contractor. The COR receives an automated electronic notification when a matter closes and barring any instructions to retain the records longer (e.g., investigative purposes), the COR will manually notify the contractor three months later. The contractor will then provide the COR with the chain of custody and Final Disposition certificate signed and dated. Records transferred back to the CFPB will then be maintained in a locked evidence locker and destroyed in accordance with the relevant records retention schedule. As noted above, the CFPB retains records in accordance with National Archives and Records Administration (NARA) General Records Schedules and NARA-approved Bureau record schedules.

Security

There is a risk of loss or unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure for information maintained in a contractor-environment. This risk is mitigated. To mitigate this risk, all CFPB staff, including federal contractors with access to CFPB information and systems are subject to the same federal laws, regulations, and policies while working at the CFPB and proceed through the same background investigations for suitability and security clearance determinations. Other requirements placed on federal contractors also include those associated with Federal Acquisition Regulations.

Bureau records are only shared with contractors that have a need to know based on job duties. CFPB records are transferred to the contractor using encrypted physical media (e.g., hard drives) or over secure File Transfer Protocol and vice versa. These records are maintained by the contractor in a FedRAMP-secured environment. All users are required to read and sign the "Employee Rules of Behavior" before being granted access. Access to the environment is strictly provided through an approval authorization process. In addition, the following access controls are in place to prevent misuse or unauthorized access to CFPB records:

- Assignment of unique account name and complex passwords;
- Multifactor authentication via PIV;
- RSA soft tokens are used for second factor authentication (if applicable);
- Automatic removal of inactive accounts;
- Least privilege access procedures; and
- Role-based access controls.

The contractor employs role-based access controls to ensure that users only have access to the environment and CFPB records maintained therein that are necessary and relevant to their assigned job duties. For example, these role-based access controls only permit a user to see or modify information for cases or matters to which they are assigned.

Finally, the contractor has established oversight controls through robust auditing features to identify and support accountability for unauthorized use/misconduct. Suspicious or unauthorized access is monitored and logged, thereby deterring users from inappropriate access and use of CFPB information. Information maintained in the audit log includes but is not limited to, the type of audit event, date and time event occurred, and user ID to identify the employee. The audit log is stored separately and protected from viewing or access by authorized users.

Document control

Approval

CHRISTOPHER CHILBERT
Digitally signed by CHRISTOPHER CHILBERT
Date: 2024.07.02 16:36:32 -04'00'

Christopher Chilbert

Chief Information Officer

KATHRYN FONG
Digitally signed by KATHRYN FONG
Date: 2024.07.02 16:40:31 -04'00'

Kathryn Fong

Chief Privacy Officer

PAUL IZZETT
Digitally signed by PAUL IZZETT
Date: 2024.07.02 10:06:28 -04'00'

Paul Izzett

Program Lead

JOSEPH CALVARESE
Digitally signed by JOSEPH CALVARESE
Date: 2024.07.02 11:06:49 -04'00'

Joe Calvarese

System Owner